



南京横渡医疗技术有限公司

防统方系统 V6. 10

技术白皮书

南京横渡医疗技术有限公司

二〇二六年三月



目录

1. 产品概述	1
2. 采购医院应用现状	2
3. 防统方系统工作原理	10
4. 防统方设备应用部署	11
5. 判断统方的依据	13
6. 自定义策略设置	14
7. 横渡防统方系统是如何区分统方行为的	15
8. 项目应用效果及社会效益	16
9. V6.10 新版特色功能截图	17
10. 售后服务承诺	25
11. 全国案例 5000+	26
12. 项目应用效果及社会效益	29
13. 技术功能规格表	30

1. 产品概述

统方:是医院对医生用药信息量的统计。

非法统方:又称为商业目的“统方”，是指医院中个人或部门为各类营销人员提供医生或部门一定时期内临床信息，供其发放商业回扣的行为。为贯彻落实卫健委《关于加强医疗卫生机构统方管理的规定》，进一步规范医疗卫生服务行为，加强行业作风建设，医院严禁为不正当商业目的统方。非正常统方行为作为药耗回扣利益链条中的重要环节，既违反了《医疗机构工作人员廉洁从业九项准则》，同时触犯了中华人民共和国刑法第 285 条第 2 款，构成非法获取计算机信息系统数据、非法控制、计算机信息系统罪，该行为破坏了医疗机构良好的公众形象，降低了医疗机构的社会满意度，因此医院需要部署控制统方的系统，并保证审查数据保存 6 个月以上。



目前医院工作的开展对信息系统的依赖性越来越强，致使信息系统越来越庞大，各业务系统关联性越来越复杂，核心数据泄密的隐患也越来越突出。

现在统方的人员和手段很多，人员有软件供应商、服务外包、数据维护人员和院内人员。

医院信息化系统中存在的隐患：非正常统方行为、居民健康档案外泄、财务数据安全。目前医院防统方的手段只局限于依赖员工职业道德并以双密码的用户

认证方式进行约束，在国内还没有任何单位能提供系统化、智能化的医院防统方服务，缺乏技术手段来杜绝医院内的统方行为。鉴于上述技术缺陷，医院迫切需要一套信息管理系统，对敏感数据进行实时监控，对违规操作进行追根溯源和智能控制。



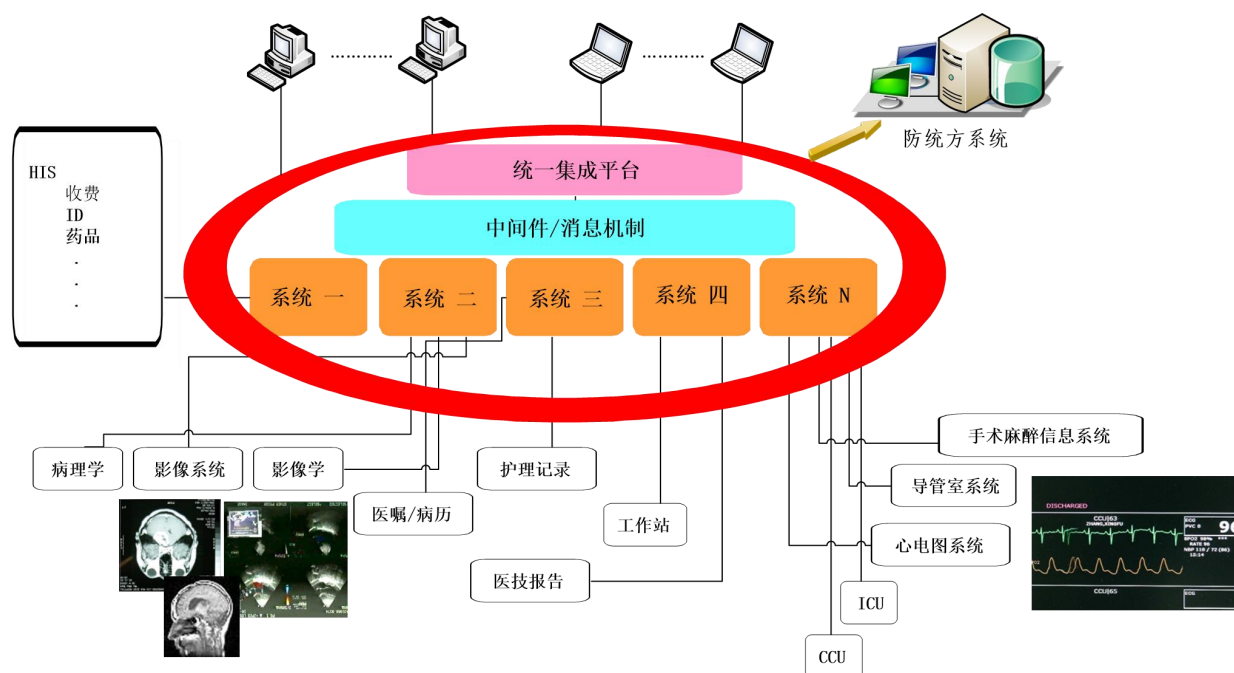
针对这一难题，南京横渡医疗技术有限公司推出了目前国内第一套的医院整体防统方系统解决方案，实现对网络和本地的所有活动，包括用户、地址、程序和操作内容进行完整全面的监控和记录，对审计记录结果能够方便的保存，检索和查询，按需审计；同时还能够对危险行为如：删除表操作，进行报警甚至阻断，并提供对数据库访问进行统计和分析，对数据库性能改进提供参考依据，使防统方手段实现了从制度约束到技术实现的跨越。为确保医药资金安全，防止利用数据库信息进行“统方”、擅自更改医院和病人信息数据等问题。横渡医院防统方系统将进一步为卫生医疗行业信息化应用保驾护航！

2. 采购医院应用现状

医院使用多家业务系统、电子病历系统以及其他应用系统都采用多层架构，结构复杂，其功能模块可以动态加载，是一个以应用为驱动的信息平台；所有数

据进行统一存储、集中展示。医院防统方系统可与平台无缝集成,对业务不产生任何影响。

随着医院不同的业务系统之间数据共享的增多,核心数据的安全成为信息安全的重点。



保护数据安全, 需要从以下几个方面考虑:

(1) 数据操作符合规范

随着中国《网络安全法》的实施, 数据安全已经成为企业信息安全中的重点。对于敏感数据做合规性审查, 及时发现嫌疑对象, 记录相关的操作信息。

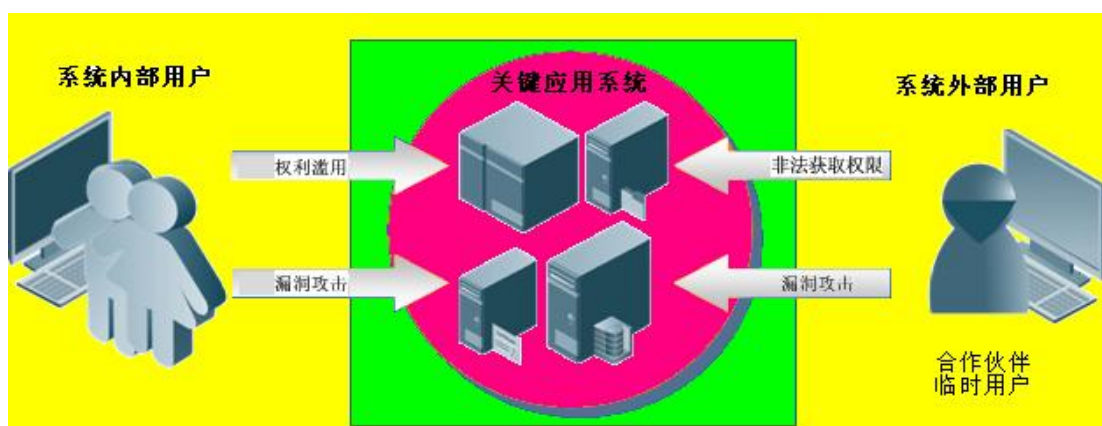


(2) 确保数据安全

核心数据是医院业务系统的基础，确保数据完整性和安全性相当重要。诸多因素包括密码安全性较差，错误的配置、未被察觉的系统后门等，使系统数据安全存在巨大隐患。

(3) 违规操作可监控

对于数据库合法用户的违规操作，非授权用户的访问，以及内部用户对关键、敏感数据资源的故意泄露或破坏等问题，对医院带来的危害会更加严重，损失也会更加巨大。



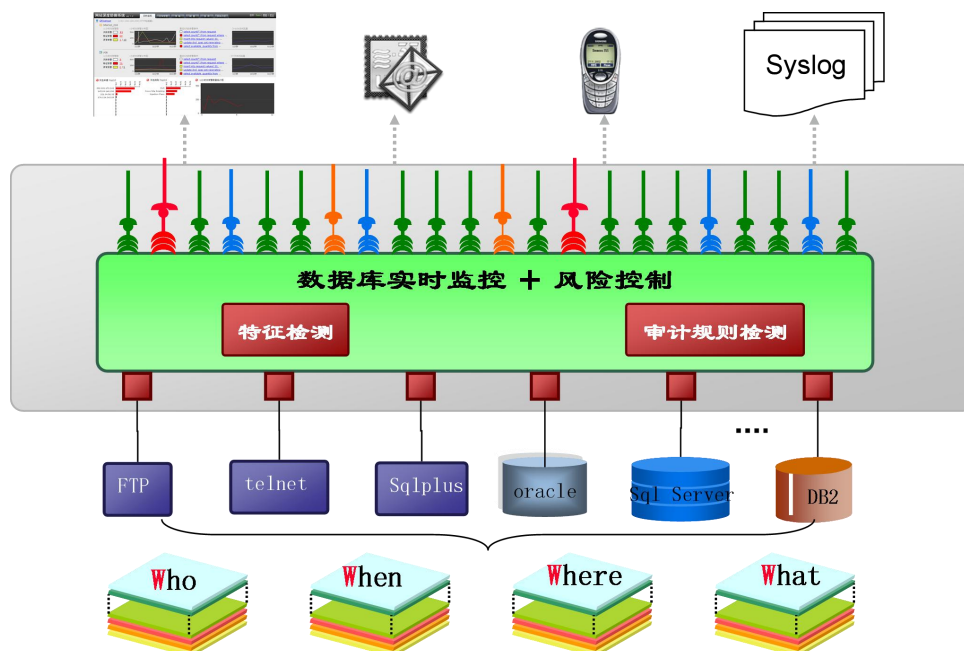
(4) 数据操作可追溯

当产生数据安全问题时，为了寻找事件线索，回溯事件过程、快速查证，具有十分重要的意义。

(5) 智能阻断数据访问

当发现核心数据被非正常访问时，及时根据预设策略阻断访问。

医院防统方系统，通过对医院核心数据的“信息活动”实时地进行监控，使管理者能够及时掌握数据的应用情况，及时发现用户的使用问题，纠正存在的安全隐患，预防应用安全事件的发生。



南京横渡医疗技术有限公司的医院防统方系统能够对网络和本地的所有活动，包括用户、时间和操作内容及方式进行完整全面的监控和记录，并对数据访问进行统计和分析，应用独特的业务活动分析技术可以区分真正的攻击与无害的用户行为变化，特有的阻断技术为数据提供实时保护，防止利用数据库信息进行“统方”、医患数据外泄、擅自篡改医院和病人信息数据等问题。系统采用加密传输机制，避免可能存在地嗅探行为，保证系统的安全。



医院防统方系统的应用流程处理通常遵循如下图所示的流程：



医院防统方系统主要使用下列方法：

- (1) 用户行为记录：记录用户所有的操作（业务访问、系统维护、策略配置等）；
- (2) 网络活动审计：采集网络数据包，通过协议解析还原网络活动并记录；
- (3) 重点监控对象：进行细粒度的行为记录与分析。
- (4) 疑似统方通知：针对可疑对象，疑似统方行为，提供多种方式实时通知。
- (5) 可疑对象定位：可以精确定位可疑对象的物理位置。
- (6) 阻断可疑会话：甄别数据访问，阻止非正常数据会话。
- (7) 行为审计报告：根据日常行为生成审计报告。



医院防统方系统从业务流程角度入手，结合核心数据特征，提供了高度集成的“事前+事中+事后”数据防护手段。

准确性

准确的内容描述，准确的人员定位，准确的结果还原

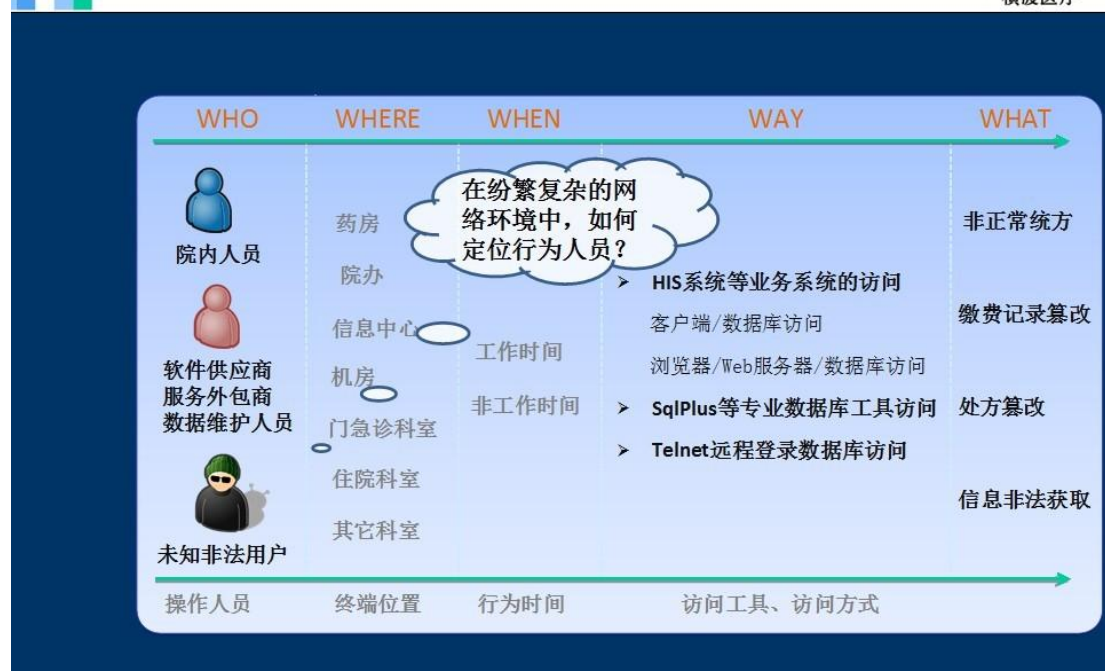
操作内容：该语句根据药品编号(ryypbm)、医生编号(ysdm)、日期(rq)等条件进行了查询(统计)操作，执行结果中包含了医生编号(ysbm)、药品数量(sl)、药品金额(ypli)等信息，对药品金额、药品数量做了累加统计操作，查询条件里面涉及到日期,范围是2011-9-25至2011-10-25，查询了药品乳果糖口服液，查询了医生系统管理员。

语句执行前后相关登录信息		
2011-10-26 14:35:36	王培培[儿科][00170]	西药库 张小凡 登录系统
2011-10-26 12:07:14	王培培[儿科][00170]	西药库 张小凡 登录系统

语句执行结果						
序号	医生姓名	药品名称	药品编号	规格	发药日期	数量
1	席大勇	乳果糖口服液	Y3562	支	2018-05-01	20
2	龚晏莹	乳果糖口服液	Y3562	支	2018-05-01	13
3	李朝霞	乳果糖口服液	Y3562	支	2018-05-01	27



防统方5+1W原则

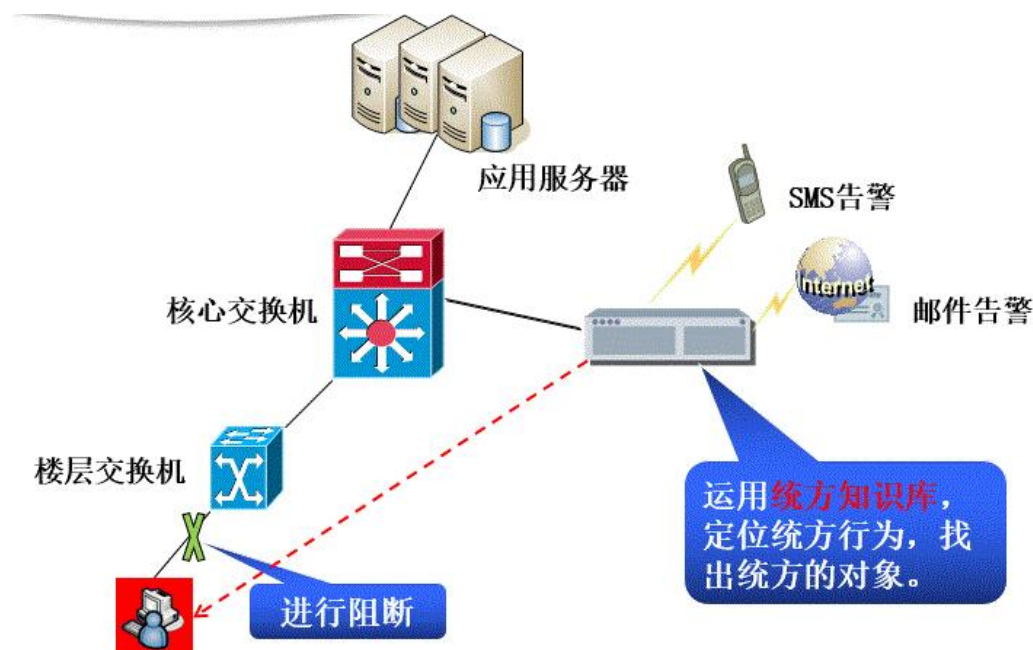




医院防统方系统可为 Oracle、MS-SQL 、DB2、MYSQL、CACHE DB、

POSTGRESQL 和 Sybase 数据库提供自动化评估、审计和保护功能。动态建模技术可自动创建数据库使用业务模型，和细化到访问系统数据库的每个用户的查询级别的安全策略。详细的数据库操作和报告功能使得查询更方便，且不会对数据库性能产生任何影响。独特的业务活动分析和相关性技术可将真正的攻击与无害的用户行为变化分离开来，从而提供实时保护。

3. 防统方系统工作原理



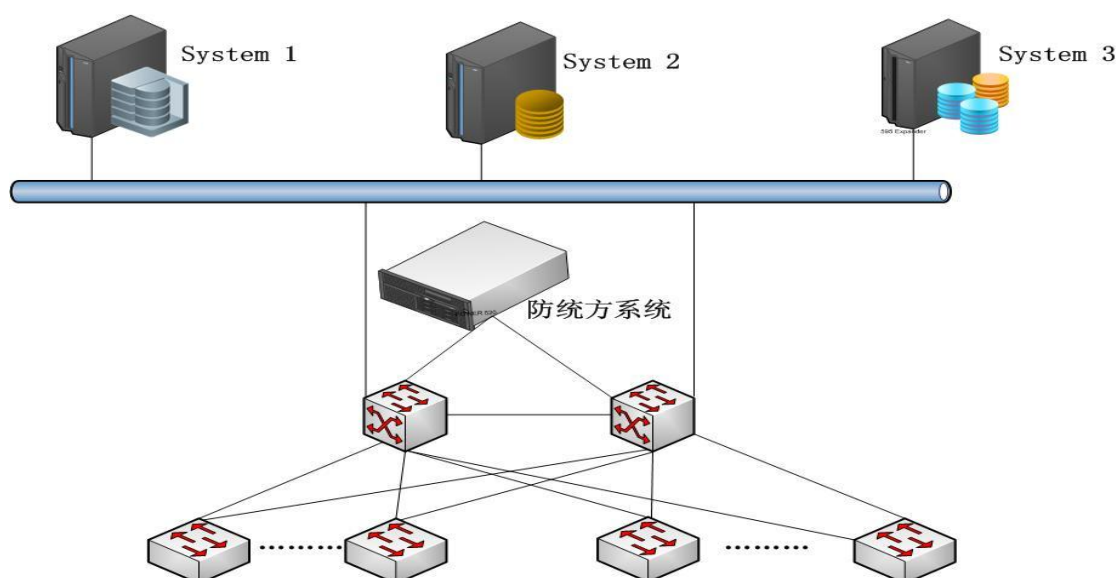
防统方系统接入医院核心交换机，镜像所有客户端发送给服务器的请求，数据同步传输至防统方系统，此时防统方系统利用自带的统方知识库对截获的数据进行分析，找出具有统方要素的行为，并对使用者进行提醒。



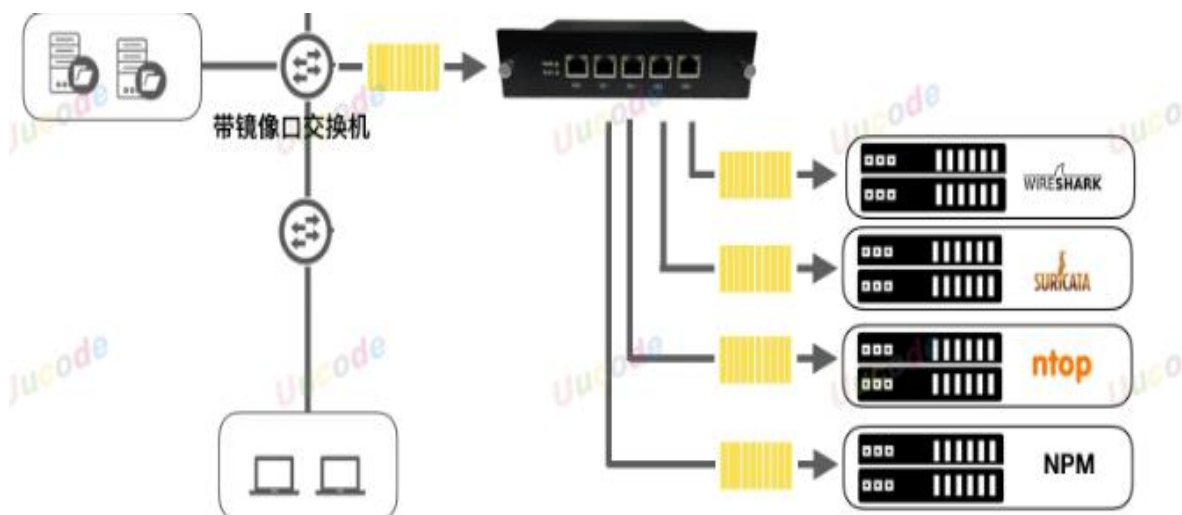
防统方能够将 web 审计记录与数据库审计记录进行关联，直接追溯到应用层的原始访问者及请求信息（如：操作发生的 URL、客户端的 IP 等信息），从而实现将威胁来源定位到最前端的终端用户的三层审计的效果。

4. 防统方设备应用部署

医院的核心网络中使用核心交换机，医院防统方系统部署在医院网络的核心层，核心交换机打开一个数据镜像端口与防统方系统进行连接，医院防统方系统接收交换机发送过来的流向各个系统的数据，进行解析、筛选、记录。

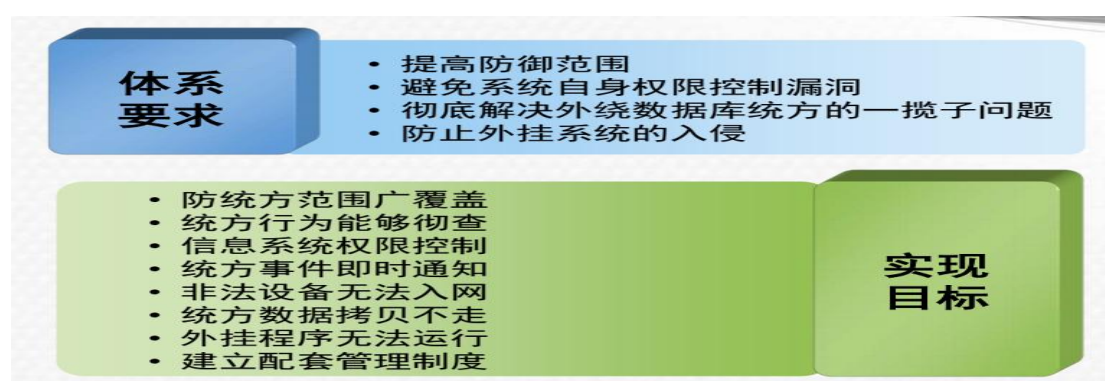


在镜像口不足时可使用 TAP 网络流量分流器，对镜像数据进行再复制分流。



通过防统方系统的解析引擎，针对所有的数据进行深度的挖掘并解析，同时结合管理员的设置，筛选记录疑似统方行为，提供访问关键系统的 IP 地址、MAC 地址、访问时间、针对系统的操作行为详细的操作内容，在一定的条件下，医院防统方系统可以根据源/目的 IP 地址、源/目的 MAC 地址、访问时间、访问内容等条件对系统访问进行阻断操作，从而达到控制客户端对非授权应用系统的访问。

对比指标	目标	审计方案
防统方范围	药品、耗材、患者信息	仅实现药品，但可扩展
统方行为追溯	完全可追溯	可实现但不完全
非法设备入网	有拦截	无限制
非法程序运行	有拦截	无限制
程序查询权限控制	可控制	无控制
系统统计数据拷走	禁止入网	未实现
直接入库查询	有审计	实现



5. 判断统方的依据

统方行为判定要素：医生、药品/高值耗材、数量/金额，时间范围。

 客户端: 192.168.2.100 [ZJ-XYK-2 制剂-西药库-2] [00-1B-FC-34-D0-69] 1

操作时间: 2011-10-26 18:32:11
使用工具: D://yyhis//doctor//bf.exe
工号: 王培培[儿科][00170]
句型类型: 危险
操作内容: 该语句根据药品编号(ryypbm)、医生编号(ysdm)、日期(rq)等条件进行了查询(统计)操作, 执行结果中包含了医生编号(ysbm)、药品数量(sl)、药品金额(yplj)等信息, 对药品金额、药品数量做了累加统计操作, 查询条件里面涉及到日期, 范围是2011-9-25至2011-10-25, 查询了药品乳果糖口服液, 查询了医生系统管理员。
当天相似操作次数: 107
[+ 语句详情](#)

单纯的一次性查询单个药品一般单位则认为其并不是在“统方”。

系统将记录该行为的相似的操作次数：

系统会将每一次操作所查询的药品一一列出。

追踪统方人员信息：

语句明细 

[设为安全](#) [设为默认](#) [设为危险](#) [句型设置](#) [发送](#) [打印](#) [▶ 执行语句](#)

基础信息 192.168.2.100					
客户端端口	客户端MAC	服务器IP	服务器端口	执行时间	操作类型
1047	00-1B-FC-34-D0-69	10.1.8.5	8106	2011-10-26 18:32:11	读取

高级信息

DB账号	工具	句型类型	句型编号	工号信息
sa	D://yyhis//doctor//bf.exe	危险	109975064	王培培[儿科][00170] 详情

涉及关键表

药房部药品派发备份(yfb_yppf_bf)、护士站处方发药明细(hsz_yz_fymx)、药房部药品处方备份(yfb_ypcf_bf)、药房部药品派发(yfb_yppf)、药房部药品处方(yfb_ypcf)

语句分析

该语句根据药品编号(ryypbm)、医生编号(ysdm)、日期(rq)等条件进行了查询(统计)操作, 执行结果中包含了医生编号(ysbm)、药品数量(sl)、药品金额(yplj)等信息, 对药品金额、药品数量做了累加统计操作, 查询条件里面涉及到日期, 范围是2011-9-25至2011-10-25, 查询了药品乳果糖口服液, 查询了

通过查看登陆情况可以准确的知道该行为的操作者是谁, 同时医院可以根据操作者的姓名得知其是否有权利去做“统方”。

6. 自定义策略设置

自定义策略设置功能提供的是医院可以根据防统方系统预警的需要，根据 IP 地址、MAC 地址、SQL 关键字、连接信息、连接信息+关键字等方式进行灵活的设置。

优先级	规则号	规则名称	状态	黑白类型	规则类型	服务器	关键字	连接信息	操作
0	6		▶	非黑即白	SQL关键字	10.3.0.100 10.3.4.103	+		修改 删除 下移
1	7		▶	黑名单	连接信息	10.3.0.100		+	修改 删除 上移 下移
2	8		▶	黑名单	连接信息	192.168.2.25		+	修改 删除 上移

例：根据 SQL 关键字设置

优先级	规则号	规则名称	状态	黑白类型	规则类型	服务器	关键字	连接信息	操作
0	6		▶	非黑即白	SQL关键字	10.3.0.100 10.3.4.103	+		修改 删除 下移
1	7		▶	黑名单	连接信息	10.3.0.100		+	修改 删除 上移 下移
2	8		▶	黑名单	连接信息	192.168.2.25		+	修改 删除 上移

多个自定义规则的组合：

优先级	规则号	规则名称	状态	黑白类型	规则类型	服务器	关键字	连接信息	操作
0	6		▶	非黑即白	SQL关键字	10.3.0.100 10.3.4.103	+		修改 删除 下移
1	7		▶	黑名单	连接信息	10.3.0.100		+	修改 删除 上移 下移
2	8		▶	黑名单	连接信息	192.168.2.25		+	修改 删除 上移

7. 横渡防统方系统是如何区分统方行为的

判断一个行为是疑似统方的行为，一般是由三个因素去判断的。第一个因素是：统方报表中的紧急告警。第二个因素是：在紧急告警中是否含有统方的几个要素包括：医生、药品、数量（金额），时间。第三个因素是：防统方软件有结果回溯功能，可以直接还原操作结果。由这三点去判断疑似统方的行为。

 客户端: 192.168.2.100 [ZJ-XYK-2 制剂-西药库-2] [00-1B-FC-34-D0-69] 1

操作时间: 2011-10-26 18:32:11
使用工具: D://yyhis//doctor//bf.exe
工号: 王培培[儿科][00170]
句型类型: 危险
操作内容: 该语句根据药品编号(ryypbm)、医生编号(ysdm)、日期(rq)等条件进行了查询(统计)操作, 执行结果中包含了医生编号(ysbm)、药品数量(sl)、药品金额(yplj)等信息, 对药品金额、药品数量做了累加统计操作, 查询条件里面涉及到日期, 范围是2011-9-25至2011-10-25, 查询了药品乳果糖口服液, 查询了医生系统管理员。
当天相似操作次数: 107
[+ 语句详情](#)

点击结果查看:

执行语句						
语句执行结果						
序号	医生姓名	药品名称	药品编号	规格	发药日期	数量
1	席大勇	乳果糖口服液	Y3562	支	2018-05-01	20
2	龚晏萱	乳果糖口服液	Y3562	支	2018-05-01	13
3	李朝霞	乳果糖口服液	Y3562	支	2018-05-01	27
4	贾凌凤	乳果糖口服液	Y3562	支	2018-05-01	55
5	崔玉芝	乳果糖口服液	Y3562	支	2018-05-01	46
6	陶小红	乳果糖口服液	Y3562	支	2018-05-01	37

回溯该操作到底是查询了什么内容。

8. 项目应用效果及社会效益

(1) 防止管理员权限滥用

能够对各级管理员的操作行为进行审计并还原出与操作相关的各项信息,且能够提供多角度、全方位报警策略制定与响应机制。

(2) 降低维护人员的安全隐患

监测维护人员的操作行为,对其操作内容进行详细记录,为统方行为的溯源提供保证。

(3) 关注业务操作风险

监测系统业务操作行为,分析业务操作流程,评估业务操作风险。

(4) 保护重要数据安全

以保障重要数据的安全为出发点,完整记录、分析对关键数据的查询、变更、删除等操作。

(5) 保障业务连续性

控制非法终端对系统的访问,保障业务连续性。

促进行风建设,提升医院形象,提高社会满意度!

9. V6. 10 新版特色功能截图

1. 产品能自定义统方规则，能够针对所有的统方特征元素包括：药品名称、医生名称、操作时间、客户端程序、IP 地址等，并能对这些元素进行与、或、非的任意逻辑组合判断。并支持结合员工工号、客户端 ip\mac 址\主机名、应用程序名和操作语句、操作时间等进行统方权限判断，非授权行为自动阻断。（可识别正常与假冒程序名，通过判断程序的 ID 编号。）

统方报表

统方参数

SQL统方参数

URL统方参数

HIS信息

报表备份

参数

任意类型

查询

新增

导出

序号	参数	类型	操作
1	physic_name	药品名称	删除
2	drug_name	药品名称	删除
3	item_name	药品名称	删除
4	drugname	药品名称	删除
5	ypmc	药品名称	删除
6	physic_code	药品编码	删除
7	drug_code	药品编码	删除
8	item_code	药品编码	删除
9	yp_code	药品编码	删除
10	ypqtdm	药品编码	删除
11	med_id	药品编码	删除
12	ypbm	药品编码	删除

« 上一页

1

2

3

4

5

下一页 »

共 59 条记录

规则类型

IP/MAC

关键字

连接信息

连接信息+关键字

IP/MAC类型

任意IPMAC

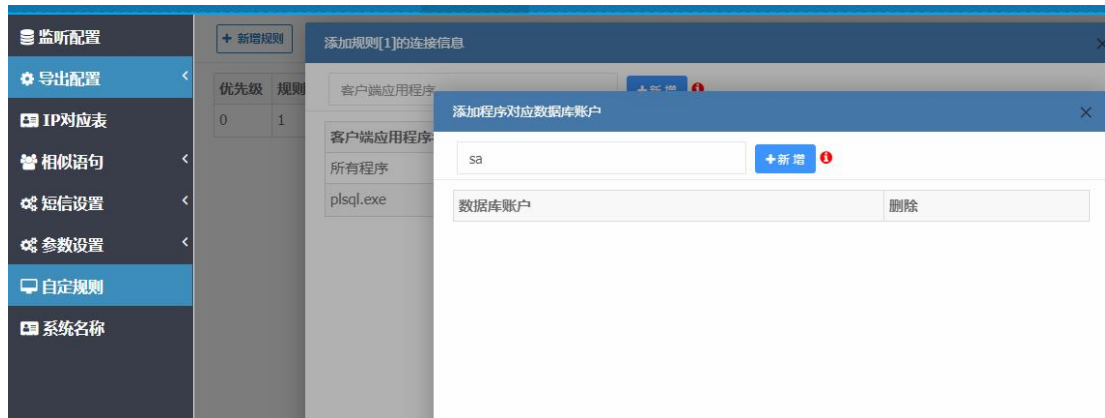
服务器IP

all

添加

删除

处理方式 ☐短信 ☐邮件 ☐告警日志 ☒ARP阻断 ☐SNMP追踪
☐桌面模块抓屏 ☒桌面模块阻断 ☐桌面模块锁屏 ☐语句单独存放

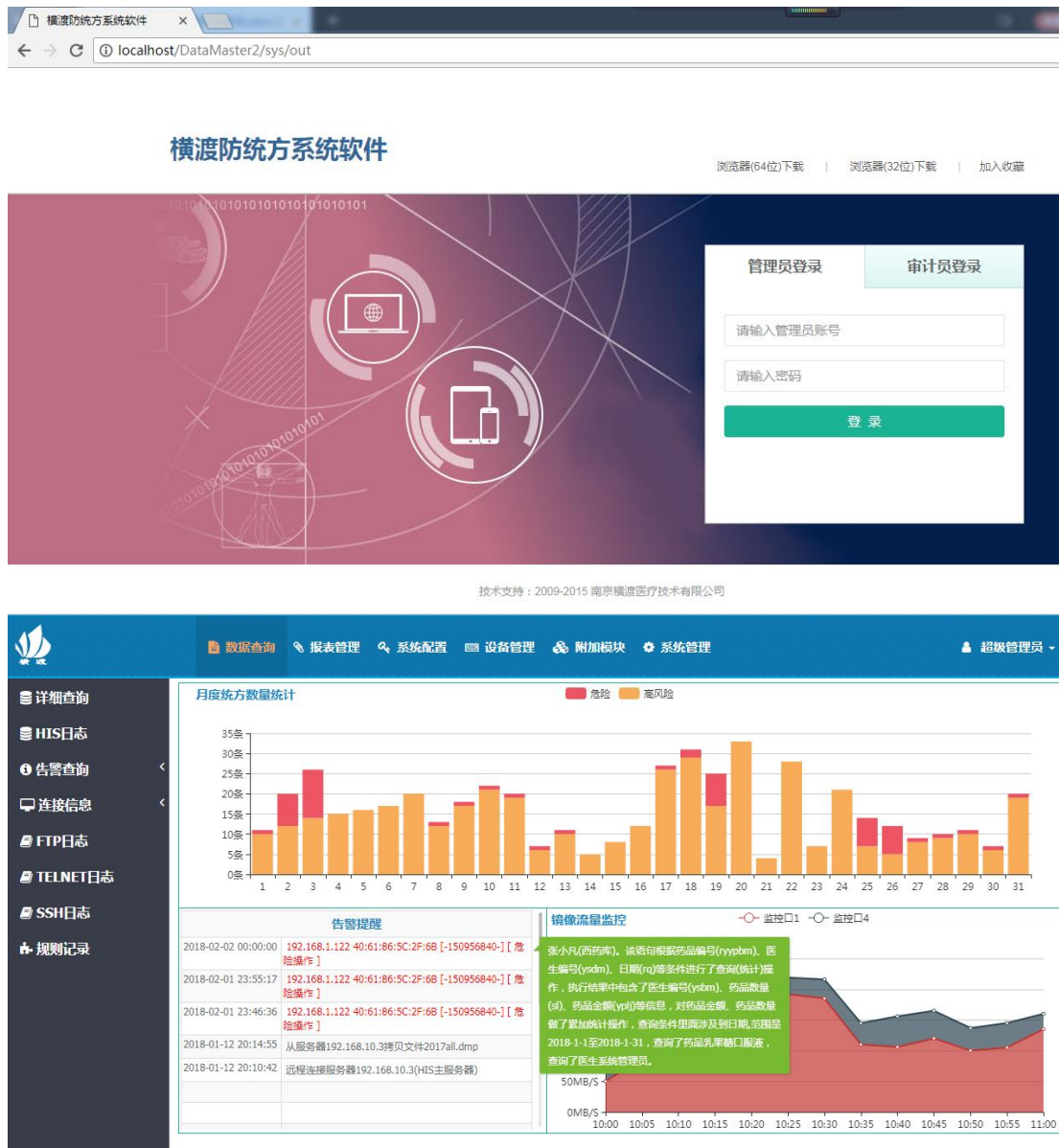


自动获取医生、药品相关信息	
药品表表名	药品表表名(或者视图名)
药品编码字段名	药品编码字段名
药品名称字段名	药品名称字段名
药品厂商字段名	药品厂商字段名
医生表表名	医生表表名(或者视图名)
医生工号字段名	医生工号字段名

2. 为了方便统方事件追踪, 必须保证审计记录完整性, 即使对于未触发统方规则的审计记录, 投标设备也需能够完整记录, 内容包括到对 HIS 数据库表的增加、删除、修改、查询、赋权、数据库链行为, 以备日后对统方事件查询分析。

新增监听			
保存 测试连接			
高级配置			
主机探针	☐	端口监听	☐
监控SQL	☒	查询语句关键字过滤	☐
非查询语句关键字过滤	☐	特殊连接信息获取功能	☐
SQL操作类型	☒ select ☒ call ☒ connect ☐ delete ☐ insert ☐ update ☐ create ☐ drop ☐ alter ☐ grant ☐ deny ☐ revoke ☐ commit ☐ rollback		
监控FTP	☐	FTP端口	21
监控TELNET	☐	TELNET端口	23
监控SSH	☐	SSH端口	22

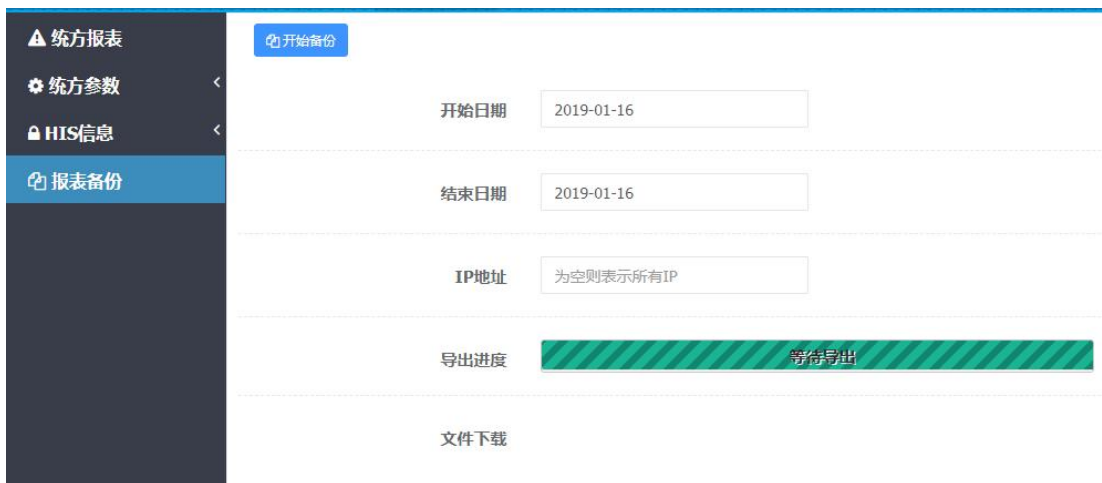
3. 用 B/S 架构，提供中文 WEB 管理界面以便于管理。并可以根据不同的安全级别采用不同的实时告警响应方式，包括 windows 消息、邮件、SNMP、录像、阻断等在内的多种响应方式。



4. 可以对某统方行为的所有操作以及操作结果关联起来，以报表的形式呈现给使用部门，便于使用部门分析和追溯统方事件。



5. 审计数据应能永久保存（请注明内接硬盘的容量大小及支持的最大容量），并支持外接存储设备进行自动压缩备份，压缩比不小于 90%。数据应进行加密保管，只能通过专门工具进行恢复和查询浏览。



（压缩成 zip 包，文本压缩率超过 90%，压缩包可设密码，压缩内容加密）

jdk1.6.0_20	2013/4/27 17:43	文件夹	
mysql	2013/4/27 17:42	文件夹	
tomcat	2013/4/27 17:42	文件夹	
1 第一步 启动数据库.bat	2013/11/28 9:05	Windows 批处理...	1 KB
2 第二步 启动网页服务.bat	2013/11/28 9:05	Windows 批处理...	1 KB
3 第三步 打开医院防统方离线查看工具	2013/11/28 9:05	Internet 快捷方式	1 KB
关闭数据库.bat	2011/3/29 14:22	Windows 批处理...	1 KB

<http://127.0.0.1:8080/DataMaster/index.jsp>

（web 形式查看工具，只有该工具可查看以上导出的备份文件）

6. 支持对 Oracle、MS-SQL、DB2、MYSQL、CACHE DB、POSTGRESQL 和 Sybase 等数据库提交自动化评估、审计和保护功能，可审计的数据库或集群数量不少于 6 个，并且可以是一个 oracle 库而另外一个其它服务器上的 SQL 数据库。

+ 新增监听							
启用	描述	监控IP	监听端口	监听类型	数据字典	服务器类型	操作
	服务器1	192.168.1.194	1433	MSSQL2008 (默认)		数据库	
	真实服务器	192.168.1.191	1521	ORACLE (gb2312)		数据库	
	备份服务器	192.168.1.192	1521	ORACLE (gb2312)		数据库	
		192.168.254.253	19725	Cache1.0 (默认)		中间件	
		192.168.254.233	1433	MSSQL2000 (默认)		数据库	
		1.1.1.1	5000	SYBASE (默认)		数据库	
		127.0.0.1	3309	MYSQL (默认)		数据库	

(同时监控的不同服务器数多达 200 个)

保存
 测试连接

基础信息			
描述	对服务器的描述或者备注	数据库类型	ORACLE
监听IP	被监听的服务器IP地址	监听端口	ORACLE
监听编码	gb2312	服务器类型	MSSQL2000

连接信息 (非必填, 正确填写可以看到语句的执行结果)

执行库IP地址	为空则默认使用监听IP	执行库端口	DB2 V9.x
账号	数据库账号	密码	SOAP
实例名	多个时用;隔开	Schema名	MIDDLEWARE
返回值编码	默认	显示行数	SOAPDYN(方案1)

(支持类型)

高级配置			
主机探针	☒	端口监听	☐
监控SQL	☒	查询语句关键字过滤	☐

(可以对服务器侦听, 保护。)

7. 支持加密方式的数据库连接信息分析 (如 MS SQL SERVER2005 及更高版本等)。

监控SQL	☐	查询语句关键字过滤	☐
非查询语句关键字过滤	☐	特殊连接信息获取功能	☒
监控FTP	☐	FTP端口	21

目前仅支持SQLSERVER2005、SQLSERVER2008, 需要配置运行功能并至少有访问master库的权限

8. 审计报告需简单明了, 且具有将计算机语言翻译成通俗易懂的自然于语言的系



统机制，支持将整条 SQL 语句翻译成中文，使卫生局中不具备计算机专业知识的人也能看懂语言，分析出是否是统方行为。

操作时间: 2011-10-26 18:32:11
使用工具: D://yyhis//doctor//bf.exe
工号: 王培培[儿科][00170]
句型类型: 危险
操作内容: 该语句根据药品编号(ryypbm)、医生编号(ysdm)、日期(rq)等条件进行了查询(统计)操作, 执行结果中包含了医生编号(ysbm)、药品数量(sl)、药品金额(yplj)等信息, 对药品金额、药品数量做了累加统计操作, 查询条件里面涉及到日期,范围是2011-9-25至2011-10-25, 查询了药品乳果糖口服液, 查询了医生系统管理员。

+ 语句详情

9. 支持医院信息管理系统多层结构，提供全方位的三层（应用层、中间层、数据库层）的访问审计，三层关联必需支持自动关联，以提升关联准确度和审计人员追踪溯源难度，同时需要支持手动关联，可以直接追踪到前端业务的操作人员 IP 地址、MAC 地址和用户。

设为安全 设为默认 设为危险 句型设置 发送 打印 结果查看

基础信息 192.168.230.113

客户端端口	客户端MAC	服务器IP	服务器端口	执行时间	操作类型
3286	00-00-00-00-03-06	192.168.254.123	80	2019-01-10 19:23:44	WEB网页

高级信息

DB账号	工具	句型类型	句型编号	工号信息
		默认	20565293	详情

语句分析

语句展示

原语句 7

/Analyzer/classes/RequestProcessor.aspx?t=11 1547193651558&xmlhttp=true&reqcmd=getPerspectives&reqparams=-357022660:CUBE_OWN:CD BI DW OWN&localeid=2052

（上图：捕获客户端发给中间层的一个方法。）

语句明细

打印

0	00-00-00-00-00-00	0.0.0.0
---	-------------------	---------

高级信息

DB账号	工具
sa	

语句分析

语句展示

原语句 1

```
select
*
from
sys_user
```

(上图:同时捕获中间层发给数据库的 SQL 语句,并把方法和 SQL 语句对应起来。)

10. 系统可以监控、记录并且还原客户端连接到服务器的 TELNET/FTP 等远程登录操作信息,防止黑客采用远程登录服务器的方式绕过防统方系统,记录内容包括客户端 IP 地址,客户端 MAC 地址,服务器地址以及产生记录的时间,对 TELNET、FTP 操作的内容回放,并提供多种查询方式。

详细查询

HIS日志

告警查询

连接信息

FTP日志

TELNET日志

SSH日志

规则记录

客户端IP

服务器IP地址

TELNET关键字

2010-01-16 00:00:00

2019-01-16 23:59:59

类型

查询

源IP	源端口	源MAC	服务器IP	TELNET命令	截获时间	操作账号	类型	返回值
172.16.1.101	1155	D4-C9-EF-D6-4A-3A	192.168.110.20	zn "dhc-app"	2017-09-13 11:49:49	root	Telnet	+明细
172.16.1.101	1155	D4-C9-EF-D6-4A-3A	192.168.110.20	sys	2017-09-13 11:49:49	root	Telnet	+明细
172.16.1.101	1155	D4-C9-EF-D6-4A-3A	192.168.110.20	_system	2017-09-13 11:49:49	root	Telnet	+明细
172.16.1.101	1155	D4-C9-EF-D6-4A-3A	192.168.110.20	cache	2017-09-13 11:49:49	root	Telnet	+明细
192.168.252.116	1645	00-00-00-00-00-01	192.168.252.114	Do company.PrintPayroll()	2017-09-13 11:49:34		Telnet	+明细

(详细列出每步执行操作内容)

11. 支持对双向数据包的解析、识别及还原,不仅对数据库操作请求进行实时监控,而且还可对数据库系统返回结果进行完整的还原,根据统方行为的特征实时告警。



语句明细							✕
执行语句							✕
语句执行结果							
序号	医生姓名	药品名称	药品编号	规格	发药日期	数量	
1	席大勇	乳果糖口服液	Y3562	支	2018-05-01	20	
2	龚晏萱	乳果糖口服液	Y3562	支	2018-05-01	13	
3	李朝霞	乳果糖口服液	Y3562	支	2018-05-01	27	
4	贾凌凤	乳果糖口服液	Y3562	支	2018-05-01	55	
5	崔玉芝	乳果糖口服液	Y3562	支	2018-05-01	46	
6	陶小红	乳果糖口服液	Y3562	支	2018-05-01	37	

10. 售后服务承诺

基本条款

- ◆ 提供系统的保修期为 36 个月；
- ◆ 在保修期内，凡因系统质量原因、我方提供的技术资料或技术指导错误造成系统损坏的，我方免费予以维护；
- ◆ 自系统保修期满之日，继续向用户提供系统的终身有偿维护服务；
- ◆ 随后续技术开发的进展，我方愿意为老用户优先提供软件版本升级及其它后续技术服务。
- ◆ 本公司为医院建立系统运行日志及档案，便于维护和及时提供系统最新安装升级，一季度巡访叁次，及时了解系统使用情况。
- ◆ 提供 7*24 小时的现场响应，提供服务热线：400-671-0088
- ◆ 如在您使用系统过程中，发生质量问题，本公司在合同规定的时间之内到达现场，处理一切问题。若 48 小时内不能修复提供备机使用。

以上承诺，本公司在履约过程中将严格执行。

11. 全国案例

11.1 南京横渡医院防统方系统已签单 5000 家医院

其中愿意公开信息的部分三级医院名单

甘肃省卫生厅及下属医院
安徽省卫生厅及下属医院
南京市卫生局及下属医院
苏州市卫生局及下属医院
徐州市卫生局及其下属医院
常熟市卫生局及下属医院
常州市卫生局及下属医院
盐城市卫生局及下属医院
连云港市卫生局及下属医院
镇江市卫生局及下属医院
绍兴市卫生局及下属医院
温州市卫生局及下属医院
上海市长宁区卫生局及下属医院
上海市徐汇区卫生局及下属医院
昆山市卫生局及下属医院
张家港卫生局及下属医院
太仓市卫生局及下属医院
吴江市卫生局及下属医院
乐清市卫生局及下属医院
宜昌市卫生局直属医院
深圳市龙岗区卫生局直属医院
江门市卫生局直属医院
广州市番禺区卫生局下属医院
惠州市卫生局下属医院

华东地区

——上海市——
复旦大学附属中山医院
上海市长宁区妇幼保健院
上海同济医院
上海市同仁医院
上海第九人民医院
上海市中西医结合医院
上海第一人民医院
上海第十人民医院

绍兴市妇幼保健院
绍兴市中医院
绍兴市文理学院附属医院
乐清市人民医院
乐清市妇幼保健院
乐清市第三人民医院
象山县第一人民医院
象山县第二人民医院
嘉善县第一人民医院
——安徽省——
安徽医科大学第一附属医院
安徽省中医院第二附属医院
安徽医科大学第二附属医院
安徽省中医院
安徽合肥市第一人民医院
安徽芜湖市第二人民医院
安徽铜陵市人民医院
安徽省池州市人民医院
安徽省皖南医学院弋矶山医院
安徽省中医学院附属针灸医院
安徽合肥市第二人民医院
安徽亳州市人民医院
安徽省立医院
安徽省立儿童医院
安徽省中医院
安徽省立友谊医院
安徽阜阳市第二人民医院
安徽安庆市第一人民医院
——福建省——
厦门大学附属第一医院
福建省三明市第二医院
——山东省——
山东省千佛山医院
济宁医学院附属医院
山东兖矿集团总医院

湖北荆门市第二人民医院
湖北省麻城市妇幼保健院
黄石中心医院
武汉市汉口医院
荆门市中医院
荆州市第三人民医院
武汉市第六医院
——湖南省——
湖南省郴州市第一人民医院
湖南省衡阳市人民医院
——河南省——
河南省中医院
河南中医学院第一附属医院
河南省中医药研究院附属医院
郑州大学第二附属医院
郑州大学第三附属医院
郑州市第二人民医院
郑州市儿童医院
新乡市中心医院
新乡市第一人民医院
洛阳正骨医院
河南科技大学第一附属医院
洛阳市妇幼保健院
济源市人民医院
商丘市第一人民医院
平顶山第一人民医院

华北地区

——天津市——
天津市西青医院
天津市宁河医院
天津市儿童医院
——北京市——
北京大学第三医院
首都医科大学附属医院



上海市东方医院
上海眼耳鼻喉科医院
上海市中山医院
上海市第九人民医院
上海曙光医院
上海青浦区中心医院
上海南汇区中心医院

——江苏省——

江苏省人民医院
江苏省肿瘤医院
南京市鼓楼医院
南京儿童医院
南京市第一人民医院
南京市口腔医院
南京市胸科医院
南京市第二人民医院
苏州大学附属第一医院
苏州大学附属第二医院
苏州市中医院
苏州市立医院
苏州市儿童医院
常州第一人民医院
常州市妇幼保健院
徐州市儿童医院
徐州市第一人民医院
徐州市第三人民医院
徐州市第四人民医院
徐州市中医院
徐州市妇幼保健院
徐州市东方人民医院
徐州市口腔医院
泰州市人民医院
泰州市中医院
无锡市人民医院
镇江市第一人民医院
镇江市第四人民医院
镇江市中医院
镇江市第三人民医院
江苏大学附属医院
苏北人民医院
淮安市第一人民医院
淮安市第二人民医院
南通市第三人民医院
江阴市中医院

潍坊市人民医院
济宁市第一人民医院
菏泽市立医院
胜利油田中心医院
枣庄市妇幼保健院
烟台市中医医院

华南地区

——广东省——

中山大学附属第一医院
中山大学附属肿瘤医院
深圳市儿童医院
广州医学院第二附属医院
广州医学院第三附属医院
深圳市儿童医院
深圳市福田区人民医院
北京大学深圳医院
汕头大学医学院附属第一医院
汕头国际眼科中心
广州市红十字会医院
广东江门市中心医院
中山大学附属口腔医院
广州中医药大学第一附属医院
番禺区中心医院
江门市中医院
广东省第二人民医院
深圳市第九人民医院
佛山市禅城中心医院
广东省佛山市中医院
广州市第一人民医院
河源市人民医院
河源市中医院
江门市新会人民医院
广东医学院附属医院
广东省人民医院
湛江市中心医院
汕头市中心医院
佛山市高明人民医院
惠州市中心人民医院
阳江市人民医院
韶关市铁路医院
佛山市中医院
东莞市人民医院
广州军区广州总医院

北京儿童医院
——河北省——
中国人民解放军二五一医院
——山西省——
山西省眼科医院
长治市妇幼保健院

西北地区

——甘肃省——

甘肃省肿瘤医院
甘肃中医学院附属医院
甘肃省康复中心医院
甘肃省武威肿瘤医院
平凉市人民医院
庆阳市人民医院
酒泉市人民医院
张掖市人民医院
兰州石化总医院
甘肃省金川公司职工医院
兰州市第二人民医院
兰州市第一人民医院

西南地区

——云南省——

云南省第二人民医院
大理大学第一附属医院
楚雄彝族自治州第二人民医院
楚雄州姚安县人民医院
昭通市中医医院
楚雄彝族自治州人民医院
楚雄州第二人民医院
昆明市第二人民医院
官渡区人民医院
昆明市呈贡区人民医院
昆明医科大学第二附属医院
陆良县人民医院
红河州第二人民医院
曲靖市第一人民医院
禄劝彝族苗族自治县第一人民医院
文山市人民医院
开远市中医院
云南省精神病医院
曲靖市中医医院
昌宁县人民医院



浙江省

浙江大学医学院附属第二医院
瑞安市人民医院
嘉兴第一医院
嘉兴市中医院
嘉兴市妇幼保健院
温州市第三人民医院
温州市中医院
温州市中西医结合医院
温州医学院附属第二医院
温州市第二人民医院
上虞人民医院
绍兴市人民医院
绍兴市第二人民医院
绍兴市第五人民医院

海南省

文昌市人民医院

广西省

广西壮族自治区人民医院
广西壮族自治区南溪山医院
广西中医药大学附属瑞康医院
桂林医学院附属医院
中国人民解放军一八一医院
玉林市第一人民医院
柳州市工人医院

华中地区

湖北省

湖北省襄阳市第一人民医院
湖北省荆州市第二人民医院
湖北荆门市第一人民医院

四川省

四川省人民医院
四川双流人民医院
重庆市
重庆西南医院
重庆市巫山县中医院
贵州省
贵州省人民医院
贵阳妇幼保健院
贵州中医第一医院

东北地区

大庆油田总医院
大连市中心医院

12. 项目应用效果及社会效益

1、防止管理员权限滥用

能够对各级管理员的操作行为进行审计并还原出与操作相关的各项信息，且能够提供多角度、全方位报警策略制定与响应机制。

2、降低维护人员的安全隐患

监测维护人员的操作行为，对其操作内容进行详细记录，为统方行为的溯源提供保证。

3、关注业务操作风险

监测系统业务操作行为，分析业务操作流程，评估业务操作风险。

4、保护重要数据安全

以保障重要数据的安全为出发点，完整记录、分析对关键数据的查询、变更、删除等操作。

5、保障业务连续性

控制非法终端对系统的访问，保障业务连续性。

促进行风建设，提升医院形象，提高社会满意度！

13. 技术功能规格表

1.1 项目描述

为贯彻落实卫健委《关于加强医疗卫生机构统方管理的规定》，进一步规范医疗卫生服务行为，加强行业作风建设，医院严禁为不正当商业目的统方。非正常统方行为作为药耗回扣利益链条中的重要环节，既违反了《医疗机构工作人员廉洁从业九项准则》，同时触犯了中华人民共和国刑法第 285 条第 2 款，构成非法获取计算机信息系统数据、非法控制、计算机信息系统罪，该行为破坏了医疗机构良好的公众形象，降低了医疗机构的社会满意度，因此医院需要部署控制统方的系统，并保证审查数据保存 6 个月以上

序号	货物名称	数量	防护区域
1	防统方系统	1 套	数据中心

1.2 产品说明

横渡防统方系统 V6.10 采用纯旁路镜像部署模式，零改造、零影响现有网络及业务系统，实现全院数据库访问行为事前预防、事中监控、事后追溯的全流程安全防护；系统适配医院多系统、多数据库、虚拟化云环境，全面满足清廉医院建设、医德医风管理及网络安全等级保护合规要求。

序号	功能模块	技术参数
1.	系统框架	1. 系统采用纯旁路审计模式，通过核心交换机镜像端口独立完成审计数据采集，无需改动现有网络结构、无需修改服务器配置、无需在业务服务器安装任何插件及程序，不依赖数据库自身审计日志，全程零影响现有网络及业务运行。 2. 管理、审计用户权限分开，相应权限的用户只能查看、管理相应的系统功能，责任明确。 3. 系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性。 4. 系统完整记录用户所有操作行为，包含业务访问、系统维护、策略配置、权限修改、报表导出等，全程留痕、全程可追溯。 5. 系统配置文件支持导入、导出。系统支持在线升级功能，通过厂家发布的升级包可在线对系统进行软件升级和规则库升级。 6. 采用 B/S 架构（兼容不同种类浏览器），提供中文 WEB 管理界面以便于管理。系统支持 HTTP 和 HTTPS 加密访问。 7. 审计数据支持归档永久保存，并支持外接存储设备进行备份（如共享文件夹、FTP）。数据进行加密保管，只能通过专门工具进行恢复和查询浏览。支持数据自动备份、手动备份。 8. 能够以图形方式显示自身使用情况。包括 CPU、内存、磁盘、IO、镜像流

		量等 9. 系统支持在线抓取指定地址、指定协议、指定数量的流量数据包，并保存为 PCAP 格式下载，供管理人员分析。 10. 系统具备用户管理功能，可以新增账号，并配置账号菜单权限。 11. 系统可以配置用户账号管理权限，包括可见的客户端范围、可见的服务器范围等。 12. 系统需具备访问限制功能，只有指定的客户端可以访问或者登录系统。 13. 系统可以设置客户单位名称、名称缩写，上传用户 LOGO，用于界面展示。 14. 支持配置登录失败次数、登录失败锁定；支持配置系统 session 失效时间。 15. 横渡防统方系统支持分布式管理及监控架构，可实现多院区、多节点统一管控。
2.	防统方模块	1. 横渡防统方系统支持 Oracle、MS-SQL、DB2、MySQL、PostgreSQL、Caché、IRIS、Sybase 等国外数据库，适配南大通用、人大金仓、达梦、神舟通用等国产数据库；支持多类型数据库并存，不限审计数据库及集群数量。 ▲2. 系统内置专业化防统方知识库，具备统方行为自主学习、规则迭代优化能力。 3. 系统可精准记录并展示操作人工号、操作类型、IP、MAC、客户端工具、系统用户名、主机名、SQL 语句、操作时间等核心信息，快速定位可疑操作终端及人员。 4. 系统支持数据库访问双向数据包解析、识别、完整还原，可同步监控请求与返回数据，精准识别隐性统方行为并截图取证。 5. 可以对接医院基础信息库，同步医生、药品、耗材等基础信息，用于界面展示，辅助客户快速判断。 ▲6. 系统支持合法统方行为线上申请、审核、报备，系统报表可标注合规报备记录，区分合规与违规操作。 ▲7. 对于确认的统方行为，系统提供归档功能，可以填写调查结果、处理结果、上传附件等相关信息。归档数据永不删除。提供专门的归档报表，供事后翻阅。 8. 系统支持按日/多日生成防统方专项审计报告，适配纪委、监察室使用；具备 SQL 语句全自动中文自然语言翻译机制，可将整条 SQL 语句转为通俗中文；支持清廉医院管理体系对接。 ▲9. 审计报告支持根据 IP 地址、服务器、工号、操作时间、风险程度、是否归档、是否报备等条件进行查询。支持按操作类型、工号、科室、IP 地址等条件进行归类。 10. 统方报告支持多种导出格式，包括但不限于 EXCEL、WORD、PDF、HTML 等。 ▲11. 系统支持按安全级别配置差异化告警方式，并支持用户自主配置告警规则，风险触发后可通过日志记录、系统消息、系统弹窗、界面鸣音、邮件、短信等方式实时推送告警信息。 ▲12. 报表免费提供公共接口，接口采用 http 接口，数据采用 JSON 格式，供医院其它系统对接用。数据内容包括但不限于告警时间、告警等级、客户端地址、服务器地址、工号、科室、操作明细、中文翻译、数据库账号等。

		13. 系统可对合理用药、互联网医院、SPD 等医院新型信息化系统开展统方审计。 14. 系统可将单次统方行为的全流程操作、执行结果自动关联整合，生成专项分析报表，支撑风险分析与责任追溯。 15. 系统适配应用层、中间层、数据库层三层架构，支持自动+手动双向关联审计，精准追溯前端操作人员及终端信息。 16. 系统支持备案统计、明细查询、审核记录追溯。详见后附证明材料。
3.	数据审计模块	1. 除统方相关操作，系统还可根据用户需求，记录非统方操作。如 create、insert、update、alert 等 DDL 操作。 2. 系统支持用户自定义审计规则，可按 IP、MAC、表名、字段、操作方式、计算机名、程序名等多条件组合查询，支持关键词模糊检索；结果支持 Excel、PDF、TXT 等格式导出。 3. 系统可以监控、记录并且还原客户端连接到服务器的 TELNET/FTP 等远程登录操作信息，记录内容包括客户端 IP 地址，客户端 MAC 地址，服务器地址以及产生记录的时间。 4. 系统支持基于 SQL 执行时长（超 30 秒）、返回/影响数据行数（≥10000 行）自定义告警规则。 5. 支持配置交换机简单网管协议 (SNMP)，支持在线查看 IP/MAC 对应表，支持在线查看系统描述、厂商标识、运行时长、运行状态等交换机信息。 6. 系统支持对应用程序、数据库访问人员、访问 IP 等信息统计；可按月统计每日数据接口流量，自动识别每月最大、最小流量对应的日期、终端、应用程序，生成可视化趋势分析图。 ▲7. 系统支持自定义非关注策略，可基于 IP、账号、程序、终端、SQL 类型、数据库表组等过滤冗余日志，降低存储压力。 ▲8. 系统支持可疑会话甄别与阻断，可基于 IP/MAC 黑名单、敏感数据内容、自定义规则，实时拦截违规 SQL 会话及访问行为。 9. 提供数据仓库功能，提高数审数据查询效率。亿级数据多条件查询速度，达到秒级。 10. 系统自动识别数据库访问应用程序，生成合法客户端清单，实时拦截非法客户端、伪装客户端的违规访问行为。 11. 系统支持基于工号、IP、MAC、客户端、操作时间、操作类型等多维度设置统方白名单，仅授权合规操作可正常访问数据库。 12. 系统深度解析数据库操作结果，支持完整操作行为回放，还原历史操作场景，满足取证溯源需求。 13. 系统支持医院财务、患者隐私、药品、耗材、资产等核心数据的全流程审计监控。 14. 系统支持账号、终端、程序、用户多维度异常探测，可配置黑白名单，对异常访问实时告警并自主优化规则。 15. 系统支持多网段客户端数据库操作会话审计，可精准追溯指定时间、终端、人员的操作行为。 16. 系统可完整解析 SQL 操作方式、表名、存储过程、执行时长、执行结果、受影响行数、关联表单等信息，完整还原原始 SQL 语句。

4.	探针模块	1. 支持通过探针，解析东华、众阳等 HTTPS 访问的 HIS 数据，记录操作行为和返回结果。 2. 支持针对服务器本机访问的监控，防止直接在服务器本机上进行统方操作。 ▲3. 系统支持虚拟化、虚拟云网络环境下的数据审计与统方行为精准定位。 ▲4. 探针必须同时支持 WINDOWS 和 Linux 操作系统，支持以服务的方式后台运行。 5. 从防统方系统上，可以直接查看探针运行情况。查看探针所在服务器状态。
	用量分析模块	▲1. 系统支持自定义统计周期，自动统计全院抗菌药物品种、剂型、规格、使用量、使用金额，生成用量、金额排名前 N 位专项报表。 2. 支持对指定时间内门诊、住院、全院药品、耗材做双十统计查询。 3. 系统支持抗菌药物数据模糊、精确多模式查询，对异常使用行为实时统计、智能告警。
6.	系统性能与硬件规格	1. 横渡防统方系统最小报警监控时间间隔 5 秒内，可极速捕捉并告警非法统方及异常数据访问行为。 2. 系统支持 2000 个客户端同时并发数据库访问监控，适配医院高并发业务场景。 3. 硬件系统吞吐量 6Gbps、SQL 处理能力 5 万条/秒、本地存储 2T、自适应电口网络接口 6 个。 4. 系统审计日志本地存储周期 180 天，满足网络安全等级保护合规溯源要求。 5. 系统对传统数据库支持 3 万字节语句完整审计，Cache 数据库支持 60 万字节语句完整审计，无日志截断缺失。
7.	安全合规与自主可控	1. 系统支持加密方式的数据库连接信息解析与行为审计，覆盖全部加密访问场景，无审计盲区。 2. 系统整体功能、日志格式、规则审计、报表输出、风险管控完全符合《网络安全等级保护基本要求》及测评规范。 3. 系统支持主动、被动双模式监控服务器开放端口，可自动扫描现有应用系统安全漏洞。
8.	医德医风与厂商关联	1. 系统捕捉非法统方行为后，可对接医院医德医风考评体系，实现年度考评“一票否决”。 2. 系统可关联非法统方对应的药品厂家、医药代表信息，实现重点标记与专项监控。

1.3 ★服务要求

- 1、 系统免费升级与维护期为三年，实施上线、维护工作由原厂厂家完成；在合同签订后 30 个工作日内完成系统开发和初验，初验后开始试运行并在试运行 30 个工作日后进行最终验收。
- 2、 提供 7*24 小时电话、现场的维护、软件升级服务；每季度提供一次巡检及协助报告



分析服务。

- 3、 免费完成与医院现有 HIS 系统数据集成对接，包含全部接口费用；对接后实现药品数据、业务报表实时同步、精准互通、无延迟、无差错。
- 4、 软件代码、数据库脚本、授权机制中无任何时间、费用、远程指令触发的锁死、禁用、数据阻断功能；项目终验后，医院拥有软件永久免费使用权，所有业务数据所有权、控制权完全归属医院，我司不限制、不扣留、不阻碍医院数据访问、导出、迁移。